



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/182,933	10/30/1998	GLENN ARTHUR REITMEIER	SAR13070	2555
28166	7590	11/21/2003	EXAMINER	
MOSER, PATTERSON & SHERIDAN, LLP /SARNOFF CORPORATION 595 SHREWSBURY AVENUE SUITE 100 SHREWSBURY, NJ 07702			MEISLAHN, DOUGLAS J	
		ART UNIT		PAPER NUMBER
		2132		29
DATE MAILED: 11/21/2003				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary**Application No.**

09/182,933

Applicant(s)

REITMEIER ET AL.

Examiner

Douglas J. Meislahn

Art Unit

2132

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 09 September 2003.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-18 and 22-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-18 and 22-29 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) The proposed drawing correction filed on _____ is: a) approved b) disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.

2. Certified copies of the priority documents have been received in Application No. _____.

3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) The translation of the foreign language provisional application has been received.

15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) Notice of References Cited (PTO-892) 4) Interview Summary (PTO-413) Paper No(s). _____ .

2) Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) Notice of Informal Patent Application (PTO-152)

3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ . 6) Other: _____

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 09 September 2003 that amended claims 1, 15, 23, and 24.

Response to Arguments

2. Applicant's arguments with respect to claims 1-14 and 24-29 have been considered but are moot in view of the new ground(s) of rejection.
3. Applicant's arguments with respect to claims 15-18, 22, and 23 filed 09 September 2003 have been fully considered but they are not persuasive. Applicant's arguments necessitate segmentation, a feature that is absent from claims 15-18, 22, and 23.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
5. Claims 1-14 and 24-29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
6. The second clauses of claims 1 and 24 dictate that the compression be done after the segmentation but then go on to say that compression is used in forming the segments. This seems contradictory in that one compression is performed at two distinct points in time: during the segmenting and after the segmenting. The examiner

has treated the claims as though "in forming said information stream segments" was deleted from the claims.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 2, 10-13, 15, and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. (5625416) in view of Kupnicki et al. (4742544) and Inoue (5195134).

In claim 1, Tseng et al. segment a video program, thereby meeting the limitations of the first clause of claim 1. As detailed in claim 4, the segments are compressed. According to claim 7, the compression is done to individual segments and thus after segmentation. MPEG, a prediction-based compression technique, is taught in lines 33-38 of column 1. As such, the limitations of the second clause of claim 1 are rendered obvious. Tseng et al. do not say that the segments are re-sequenced or encrypted. In their abstract, Kupnicki et al. teach randomly reordering segments of data in order to protect the data as a whole. Decryption data is used to reorder the re-sequenced data and thus corresponds to applicant's index. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect Tseng et al.'s segmented data by randomly re-sequencing it according to an index. Thus, the third clause of claim 1 is covered.

Encrypting data that has already been scrambled, although perhaps not a ubiquitous practice, is known in the art of data transmission, as evidenced by lines 18-22 of column 3 in Inoue; the encryption has the obvious advantage of providing increased security to the data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to increase security by encrypting Tseng et al.'s now-re-sequenced data as taught by Inoue.

An apparatus to produce this encrypted, scrambled, compressed data stream is inherent. A method to recover the data is anticipated as well.

With respect to claim 2, Inoue has taught encryption of the entire signal. Inoue also talks about subscribers in line 26 of column 3, thereby meeting the limitations of 2.

9. Claim 3, 6, 16, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claim 2 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. Control data for the mixing is also encrypted. They do not teach sending the control data to a receiver via a different medium. Official notice is taken that it is old and well known to send control data separately from the actual information. This is especially established in pay television systems; a card will be sent to a client, who puts the card in a machine on the client's television. The data on the card allows the descrambling of broadcast programming. This method provides a level of security by separating the scrambled data from the key to that data. All of the base references are concerned with data transmission, and therefore it would have

been obvious to a person of ordinary skill in the art at the time the invention was made to send control data by a different medium, such as a mailed card as is known in the art, the recipient in the combined system of Tseng et al. in view of Kupnicki et al. and Inoue. This would increase security.

10. Claims 4, 5, 17, 27, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claims 2, 3, 16, 25, and 26 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not teach non-continuous temporal transmission. Official notice is taken that transmission of data, particularly encrypted data, in a non-continuous fashion is old and well known. By providing only part of a cryptogram, an attacker (probably) cannot decrypt any of the cryptogram. This is used in the interlock protocol, which, although concerned specifically with public keys, is applicable to symmetric cryptography. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to increase the security of Tseng et al. in view of Kupnicki et al. and Inoue by transmitting the data discontinuously. Also, if the data is transmitted as packets, it would inherently be transmitted discontinuously.

11. Claims 7, 8, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claims 1 and 28 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. There is no mention in either reference of the segments being a specific size or distributing the segments over many different distribution channels. Official notice is taken that digital broadcast over computer networks is old and well known as a method for data transmission. Data is generally conveyed in packets that are generally the same size, meeting the limitations of claim 7. The networks use many different transmission paths to deliver data to a single source, meeting claim 29. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teachings of Tseng et al. in view of Kupnicki et al. and Inoue's joint transmission system to digital broadcast over networks.

12. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claim 1 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not say that a non-predicted information segment is included in the segment. Official notice is taken that it is old and well known to include random information, such as an initialization vector, in data that is to be encoded. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a non-predicted information frame within each segment of Tseng et al. in view of Kupnicki et al. and Inoue, thereby providing an initialization vector for the stream.

13. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claim 1 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not say that the step of compressing produces control information indicative of a utilization level of a decoder buffer. This feature has been interpreted as being access rights for decompression. Official notice is taken that access rights are an old and well-known type of control data that are used to indicate parties that are allowed to access a product. They are especially common in pay-television systems. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for commonly known access rights to be included in the control data of Tseng et al. in view of Kupnicki et al. and Inoue. The time of access rights generation is substantially inconsequential, but it would have been obvious to produce the rights at the same time as the operation that they control.

14. Claims 18 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claim 15 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not specifically teach storing the unencrypted data in random access memory. Official notice is taken that it is old and well known that random access storage allows a processor to directly access data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use random access memory to store the data used in Tseng

et al. in view of Kupnicki et al. and Inoue because the data is not accessed in the order in which it is meant to be viewed or heard.

15. Claims 15 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oshima et al. (WO98/27553) (US 6266299 is an English-language equivalent) in view of the Microsoft Press *Computer Dictionary* and Inoue (5195134).

Figure 34 of Oshima et al. shows data being MPEG encoded (element 43) and scrambled by a scrambler (element 45) using a key (element 44). (For translation, see English-language equivalent US 6266299 B1, figure 34 and the paragraph spanning columns 36 and 37). MPEG anticipates prediction-based compression, and the key corresponds to applicant's index. Oshima et al. do not say that the scrambling reorders data. The Microsoft Press Computer Dictionary (3rd ed.) defines a scrambler as a "device or program that reorders a signal sequence in order to render it indecipherable." As such, it would have been obvious to a person of ordinary skill in the art at the time the invention was made for Oshima et al.'s scrambler to reorder the MPEG-compressed data because, definitionally, that is what scramblers do.

Oshima et al. do not encrypt the scrambled data. Encrypting data that has already been scrambled, although perhaps not a ubiquitous practice, is known in the art of data transmission, as evidenced by lines 18-22 of column 3 in Inoue; the encryption has the obvious advantage of providing increased security to the data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the data on disks (element 240) pictured in figure 41 of Oshima et al. as taught by Inoue. This would increase security.

16. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Oshima et al. in view of the Microsoft Press *Computer Dictionary* and Inoue as applied to claim 15 above.

Oshima et al. in view of the Microsoft Press *Computer Dictionary* and Inoue render obvious a system that compresses, mixes, and encrypts data. Control data for the mixing is also encrypted. They do not teach sending the control data to a receiver via a different medium. Official notice is taken that it is old and well known to send control data separately from the actual information. This is especially established in pay television systems; a card will be sent to a client, who puts the card in a machine on the client's television. The data on the card allows the descrambling of broadcast programming. This method provides a level of security by separating the scrambled data from the key to that data. Walker et al. and Inoue are both concerned with data transmission, and therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send control data by a different medium, such as a mailed card as is known in the art, the recipient in the combined system of Oshima et al. in view of the Microsoft Press *Computer Dictionary* and Inoue. This would increase security.

17. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Oshima et al. in view of the Microsoft Press *Computer Dictionary* and Inoue as applied to claim 16 above.

Oshima et al. in view of the Microsoft Press *Computer Dictionary* and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not

teach non-continuous temporal transmission. Official notice is taken that transmission of data, particularly encrypted data, in a non-continuous fashion is old and well known. By providing only part of a cryptogram, an attacker (probably) cannot decrypt any of the cryptogram. This is used in the interlock protocol, which, although concerned specifically with public keys, is applicable to symmetric cryptography. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to increase the security of Oshima et al. in view of the Microsoft Press *Computer Dictionary* and Inoue by transmitting the data discontinuously. Also, if the data is transmitted as packets, it would inherently be transmitted discontinuously.

18. Claims 18 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oshima et al. in view of the Microsoft Press *Computer Dictionary* and Inoue as applied to claim 15 above.

Oshima et al. in view of the Microsoft Press *Computer Dictionary* and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not specifically teach storing the unencrypted data in random access memory. Official notice is taken that it is old and well known that random access storage allows a processor to directly access data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use random access memory to store the data used in Oshima et al. because the data is not accessed in the order in which it is meant to be viewed or heard.

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Nguyen et al. (6529553) – figure 5 and related description in lines 8-18 of column 3; Ginzboorg et al. (6349088) – lines 65-67 of column 1; Imai (6035068) – abstract; Katz et al. (5926624) – figure 3 and the first paragraph of column 6; Jerkunica et al. (5802520) – field of the invention and the paragraph spanning columns 1 and 2, especially lines 65-67 of column 1; Craft (5764994) – abstract; Ramchandran et al. (5734755) – lines 7-8 of column 2; Pan et al. (5701391) – lines 41-44 of column 5; and Ibaraki et al. (5546461) – figures 1 and 3.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.


Douglas J. Meislahn
Examiner
Art Unit 2132

DJM